



REPLY TO  
ATTENTION OF

**DEPARTMENT OF THE ARMY**  
HEADQUARTERS, U.S. ARMY GARRISON VICENZA  
UNIT 31401, BOX 80  
APO AE 09630

IMEU-VIC-IA

24 February 2006

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: U.S. Army Garrison Vicenza Policy No. 06-41, Computer User Policy

1. Reference AR 25-2, Information Assurance, 14 November 2003.
2. This policy applies to all military, civilians, and local national employees within the U.S. Army Garrison (USAG) Vicenza and USAG Livorno.
3. All government computer **users** within the USAG Vicenza, and USAG Livorno will adhere to the following computer user rules:
  - a. All computers will be **left-on** unless otherwise instructed by your Information Assurance Security Officer (IASO), Information Management Officer (IMO), or the Garrison Information Assurance Manager (IAM). At the end of the day, just **re-start** your computer and leave it **on** (*do not log back-in*). **Turn-off** all monitors, and other peripherals, i.e. printers, facsimiles, etc, at the end of the working day. Re-starting your computer will allow for any security updates to register on your computer, and minimizes your computer of being vulnerable to viruses, worms, Trojan Horses, etc. If a computer scan reveals that your computer is vulnerable due to the system being off when a security patch was pushed, your computer will be disabled from the network and will not be turned back-on until it is safe to connect back to the network. You will need to put a work order through our help desk to get your computer back on the network. Due to other high priorities and limited Information Technology specialist, do not expect your computer to be fixed right away. **BE SURE YOU LEAVE YOUR COMPUTER ON AT THE END-OF- DAY, WHEN ON LEAVE, TDY, ETC!**
  - b. **LAPTOPS/NOTEBOOKS.** All Laptops and Notebooks should stay connected to the network when not on TDY. This will allow your system to stay up-to-date and virus protected. If your Laptop or Notebook computer have not been connected to the USAREUR network for more than a week, you **must** take your system to your IMO/IASO before connecting it back to the network. **KEEP YOUR COMPUTER CONNECTED TO THE NETWORK WHEN IN TOWN!**

IMEU-VIC-IA

SUBJECT: U.S. Army Garrison Vicenza Policy No. 06-41, Computer User Policy

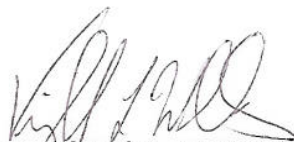
c. Use of commercial e-mail services, i.e., HOTMAIL, YAHOO, AOL, etc. **is not** authorized on government computers. You may use AKO e-mail services for personal e-mails and chatting services. Downloading freeware or Shareware **is not** authorized on our network. Use of unauthorized software potentially poses a threat to our network. Your IASO/IMO/IAM must authorize any software you might need to perform your job. **DO NOT DOWNLOAD UNAUTHORIZED PROGRAMS ON GOVERNMENT COMPUTERS!**

d. Prohibited websites. Users will not visit any websites dealing with pornography, or any other sites that promulgates hates, or racial discrimination. Even though USAREUR have a program in placed (WEBSense) to block these types of websites there is always the possibility of new sites this program have not picked up yet. **YOU DO NOT WANT TO BE THE SUBJECT OF AN INVESTIGATION!**

e. Sensitive Information. All sensitive but unclassified information must be sent via secure media. Secure media ranges from encrypted e-mail (PKI) to using approved classified systems, i.e. computers, secure fax, etc. Your IMO/IASO can provide guidance on acquiring PKI enabling to include local nationals that may required to process sensitive information on a regular due to the nature of their duties. **ALL MILITARY AND DOD CIVILIANS MUST BE PKI CERTIFIED!**

f. Reminder. Regulation 25-2, Information Assurance, is punitive in nature, and empowers commanders to enforce disciplinary actions against violators of paragraph 3. a. thru e. stated on this memorandum. Military personnel are subject to UCMJ, and civilian punishment can range from administrative sanctions to loosing your job. **PROTECT YOUR JOB BY AVOIDING BECOMING A SUBJECT OF THIS TYPE OF INVESTIGATION!**

5. The point of contact for this issue is Ms. Prados, Information Assurance Manager, 634-8222, e-mail: [juana.prados@setaf.army.mil](mailto:juana.prados@setaf.army.mil).

  
VIRGIL S.L. WILLIAMS  
COL, QM  
Commanding

DISTRIBUTION:

United States Army Garrison Vicenza

Directorate of Plans, Training, Mobilization & Security

IMEU-VIC-IA

SUBJECT: U.S. Army Garrison Vicenza Policy No. 06-41, Computer User Policy

Directorate of Human Resources  
Directorate of Morale, Welfare & Recreation  
Directorate of Logistics  
Directorate of Public Works  
Directorate of Emergency Services  
Directorate of Resource Management  
Plans, Analysis & Integration Office  
Safety Office  
Equal Opportunity  
Chaplain Office  
Public Affairs Office  
School Liaison Officer  
United States Army Garrison Livorno